UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/667,752	09/22/2003	Roger John O'Hara	14846-14	4808

7590 10/17/2007

MICHAEL B. JOHANNESEN, ESQ.
LOWENSTEIN SANDLER, P.C.
65 LIVINGSTON AVENUE
ROSELAND, NJ 07068

EXAMINER	
BELANI, KISHIN G	

ART UNIT	PAPER NUMBER
2143	

MAIL DATE	DELIVERY MODE
10/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/667,752	O'HARA, ROGER JOHN	
	Examiner	Art Unit	
	Kishin G. Belani	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,9-11 and 13-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,9-11 and 13-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to Applicant's amendment filed on 8/30/2007. **Independent claims 1 and 11 have been amended. Dependent claims 4 and 9 have been amended** to correct minor informalities. As a result, objection to claim 4 and 112 second paragraph rejection for claim 9 have been withdrawn. **Claims 6-8 and 12 have been cancelled. New Independent claims 17 and 18 have been added. Claims 1-5, 9-11 and 13-18 are now pending** in the present application. The applicants' arguments are shown in ***bold and italics***, and the examiner's response to the arguments is shown in **bold** in this office action. **This Action is made FINAL.**

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness

or nonobviousness.

Claims 1-5, 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Carley (U.S. Patent Application Publication # 2003/0233583 A1),** in view of **Grieve et al. (U.S. Patent Application Publication # 2003/0149756 A1).**

Consider **claim 1**, Carley shows and discloses a method for securely managing and monitoring a data network, said data network comprising a plurality of network components (Abstract that discloses a network management system for remotely and securely managing a data network; Fig. 17, SRMA (Secure Remote Management Appliance) block along with a plurality of network components (router, servers, and network management station), said method comprising:

connecting a network management system to a non-network port of each of said network components (paragraphs 0088 and 0089 which disclose that the network management connection can be via the console port (as an RS-232 serial interface) of the network element);

managing each of said network components through said non-network port (paragraph 0002 which discloses that the invention relates to managing devices or elements in a communication network); and

monitoring each of said network components through said non-network port (paragraph 0021 which states that monitoring network connections for possible attacks and reporting them to Intrusion Detection System is one of the objective of the invention).

However, in the claimed method, Carley does not disclose ***wherein monitoring each of the network components comprises periodically sampling the network configuration of each of the network components by the system monitor, and comparing the sampled network configurations to stored network configurations at the network management system.***

In the same field of endeavor, Grieve et al. disclose the claimed method ***wherein monitoring each of the network components comprises periodically sampling the network configuration of each of the network components by the system monitor, and comparing the sampled network configurations to stored network configurations at the network management system*** **(Abstract that discloses a method for periodically comparing two different configuration files created at different times, thereby disclosing periodically sampling and comparing configurations of network components for monitoring purposes; paragraph 0007 discloses the same details, specifically lines 8-12 that disclose periodically sampling and comparing; paragraph 0033 that discloses a software agent 104 shown in Fig. 1, which acts as a system monitor)**.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to disclose that monitoring each of the network components comprises periodically sampling the network configuration of each of the network components by the system monitor, and comparing the sampled network configurations to stored network configurations at the network management system, as

taught by Grieve et al., in the method of Carley, so that the integrity of the network can be periodically verified.

Consider **claim 2**, and **as applied to claim 1 above,** Carley, as modified by Grieve et al., further shows and discloses a method wherein connecting a network management system to a non-network port of each of said plurality of network components comprises: connecting a network management system to a terminal server (Fig. 17, SRMA block that acts as a terminal server, connecting each of the plurality of network components (router, servers etc.) of a data network via their non-network ports to the Network Management Station; paragraph 0089 which discloses that the SRMA can have multiple connections for accessing device consoles, thus acting like a terminal server); and

connecting said terminal server to said non-network port of each of said network components (paragraphs 0088 and 0089 which disclose that the SRMA connects to the network components via non-network port of each component).

Consider **claim 3**, and **as applied to claim 2 above,** Carley as modified by Grieve et al., further discloses a method further including establishing communication between said network management system and said terminal server via TCP/IP (paragraph 0090 which discloses that the access to a dedicated network segment of network management can be Ethernet or Fast Ethernet (TCP/IP).

Consider **claim 4**, and **as applied to claim 2 above,** Carley as modified by Grieve et al., further discloses a method further including establishing communication between said terminal server and said plurality of network components via RS-232 serial interface (paragraph 0089 which discloses that the access to the console port of a network element is via an RS-232 serial interface).

Consider **claim 5**, and **as applied to claim 1 above**, Carley as modified by Grieve et al., further shows and discloses a method wherein said network management system includes a configuration manager (Fig. 17; paragraph 0117 which discloses that the router configuration transmitted by the system administrator via the network is encrypted by the SRMA, thereby disclosing a configuration manager), said method further comprising: configuring said plurality of network components from said configuration manager through said non-network port of each of said network components (paragraph 0089 which discloses that the access to the console port of a network element is via an RS-232 serial interface).

Consider **claim 17**, Carley shows and discloses ***a method for securely managing and monitoring a data network, said data network comprising a plurality of network components*** **(Abstract that discloses a network management system for remotely and securely managing a data network; Fig. 17, SRMA (Secure Remote Management Appliance) block along with a plurality of network**

components (router, servers, and network management station), *said method comprising:*

***connecting a network management system to a non-network port of each of said network components* (paragraphs 0088 and 0089 which disclose that the network management connection can be via the console port (as an RS-232 serial interface) of the network element);**

***managing each of said network components through said non-network port* (paragraph 0002 which discloses that the invention relates to managing devices or elements in a communication network);**

***monitoring each of said network components through said non-network port* (paragraph 0021 which states that monitoring network connections for possible attacks and reporting them to Intrusion Detection System is one of the objective of the invention).**

However, in the claimed method, Carley does not disclose ***wherein managing each of said network components comprises deploying a network configuration of each of the network components from stored network configurations at the network management system.***

In the same field of endeavor, Grieve et al. disclose the claimed method ***wherein managing each of said network components comprises deploying a network configuration of each of the network components from stored network configurations at the network management system*** **(paragraph 0007, lines 12-16 which disclose identifying as representing a known good state, an earlier stored**

second configuration file; and recommending returning to the known good state by loading the second configuration file, when the difference is indicated).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to disclose that managing each of said network components comprises deploying a network configuration of each of the network components from stored network configurations at the network management system, as taught by Grieve et al., in the method of Carley, so as to provide means for recovering from a faulty update to the configuration file of a network component.

Consider **claim 18**, Carley shows and discloses ***a method for securely managing and monitoring a data network, said data network comprising a plurality of network components*** **(Abstract that discloses a network management system for remotely and securely managing a data network; Fig. 17, SRMA (Secure Remote Management Appliance) block along with a plurality of network components (router, servers, and network management station),** ***said method comprising:***

connecting a network management system to a non-network port of each of said network components **(paragraphs 0088 and 0089 which disclose that the network management connection can be via the console port (as an RS-232 serial interface) of the network element);**

managing each of said network components through said non-network port **(paragraph 0002 which discloses that the invention relates to managing devices or elements in a communication network);**
monitoring each of said network components through said non-network port **(paragraph 0021 which states that monitoring network connections for possible attacks and reporting them to Intrusion Detection System is one of the objective of the invention).**

However, in the claimed method, Carley does not disclose ***wherein monitoring each of the network components comprises periodically sampling the network configuration of each of the network components by the system monitor, and comparing the sampled network configurations to stored network configurations at the network management system; and wherein managing each of said network components comprises deploying a network configuration of each of the network components from stored network configurations at the network management system.***

In the same field of endeavor, Grieve et al. disclose the claimed method ***wherein monitoring each of the network components comprises periodically sampling the network configuration of each of the network components by the system monitor, and comparing the sampled network configurations to stored network configurations at the network management system*** **(Abstract that discloses a method for periodically comparing two different configuration files created at different times, thereby disclosing periodically sampling and comparing**

configurations of network components for monitoring purposes; paragraph 0007 discloses the same details, specifically lines 8-12 that disclose periodically sampling and comparing; paragraph 0033 that discloses a software agent 104 shown in Fig. 1, which acts as a system monitor)*; and*

wherein managing each of said network components comprises deploying a network configuration of each of the network components from stored network configurations at the network management system **(paragraph 0007, lines 12-16 which disclose identifying as representing a known good state, an earlier stored second configuration file; and recommending returning to the known good state by loading the second configuration file, when the difference is indicated).**

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to disclose that monitoring each of the network components comprises periodically sampling the network configuration of each of the network components by the system monitor, and comparing the sampled network configurations to stored network configurations at the network management system; and wherein managing each of said network components comprises deploying a network configuration of each of the network components from stored network configurations at the network management system, as taught by Grieve et al., in the method of Carley, so as to periodically verify the integrity of the network and provide means for recovering from a faulty update to the configuration file of a network component.

Claims 9-11 and 13-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Carley (U.S. Patent Application Publication # 2003/0233583 A1),** in view of **Grieve et al. (U.S. Patent Application Publication # 2003/0149756 A1)** and further in view of **Cambron (U.S. Patent Publication # 6,539,027 B1).**

Consider **claim 9**, and **as applied to claim 1 above,** Carley as modified by Grieve et al., shows and discloses the claimed invention including showing a terminal server connected between said network management system and said plurality of network components (in Carley reference, as detailed in claim 1 above and shown in Fig. 17).

However, Carley as modified by Grieve et al., does not explicitly show a method wherein said step of monitoring each of said plurality of network components comprises polling each of said plurality of network components by said terminal server responsive to a system monitor.

In the same field of endeavor, Cambron clearly discloses that monitoring each of said plurality of network components comprises polling each of said plurality of network components by said terminal server responsive to a system monitor (column 7, lines 40-53 which disclose that SNMP network-management architecture includes a SNMP manager (system monitor), that enables the network administrator to carry out network management functions by regularly polling and monitoring all SNMP devices in a network).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to monitor each of said plurality of network components by polling each of said plurality of network components by said terminal server responsive to a system monitor, as taught by Cambron in the method of Carley, as modified by Grieve et al., so that the network administrator can perform network management functions, such as fault, configuration, security, performance and accounting management at regular intervals.

Consider **claim 10**, and **as applied to claim 1 above,** Carley as modified by Grieve et al., shows and discloses the claimed invention except initiating communication between said network management system and said plurality of network components only from said network management system.

In the same field of endeavor, Cambron clearly discloses initiating communication between said network management system and said plurality of network components only from said network management system (column 7, lines 40-53 which disclose that SNMP network-management architecture includes SNMP agents, which interact with the devices being managed, and which enable a management station to poll all SNMP devices in the network in order to initiate communication for the purpose of network management).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to monitor and poll each of said plurality of network components for the purpose of initiating communication between said network

management system and said plurality of network components only from said network management system, as taught by Cambron in the method of Carley, as modified by Grieve et al., so that the network management functions, such as fault, configuration, security, performance and accounting management can be performed at regular intervals.

Consider **claim 11**, Carley shows and discloses an apparatus (SRMA (Secure Remote Management Appliance)) for secure monitoring of network components in a data network (Abstract that discloses a network management system for remotely and securely managing a data network) comprising:
a plurality of network components (Fig. 17, with a plurality of network components (router, servers, and network management station)),
each of said plurality of network components having a data network port connected to said data network and each of said plurality of network components having a non-network port (paragraphs 0088 and 0089 which disclose that the network management connection can be via the console port (as an RS-232 serial interface) of the network element).

However, Carley does not explicitly disclose a network management system connected to each of said plurality of network components at said non-network port and configured so that only said network management system may initiate communication with said plurality of network components***; wherein monitoring each of the network components comprises periodically sampling the network configuration of each***

of the network components by the system monitor, and comparing the sampled network configurations to stored network configurations at the network management system.

In the same field of endeavor, Grieve et al. disclose an apparatus ***wherein monitoring each of the network components comprises periodically sampling the network configuration of each of the network components by the system monitor, and comparing the sampled network configurations to stored network configurations at the network management system*** **(Abstract that discloses a system for periodically comparing two different configuration files created at different times, thereby disclosing periodically sampling and comparing configurations of network components for monitoring purposes; paragraph 0007 discloses the same details, specifically lines 8-12 that disclose periodically sampling and comparing; paragraph 0033 that discloses a software agent 104 shown in Fig. 1, which acts as a system monitor)**.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to disclose that monitoring each of the network components comprises periodically sampling the network configuration of each of the network components by the system monitor, and comparing the sampled network configurations to stored network configurations at the network management system, as taught by Grieve et al., in the apparatus of Carley, so that the integrity of the network can be periodically verified.

However, Carley, as modified by Grieve et al., does not explicitly disclose a network management system connected to each of said plurality of network components at said non-network port and configured so that only said network management system may initiate communication with said plurality of network components.

In the same field of endeavor, Cambron discloses an apparatus with a network management system connected to each of said plurality of network components at said non-network port and configured so that only said network management system may initiate communication with said plurality of network components (column 7, lines 40-53 which disclose that SNMP network-management architecture includes SNMP agents, which interact with the devices being managed, and which enable a management station to poll all SNMP devices in the network in order to initiate communication for the purpose of network management).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide a network management system connected to each of said plurality of network components at said non-network port and configured so that only said network management system may initiate communication with said plurality of network components, as taught by Cambron in the apparatus of Carley, as modified by Grieve et al., so that the network management functions, such as fault, configuration, security, performance and accounting management can be performed at regular intervals.

Consider **claim 13**, and **as applied to claim 11 above,** Carley as modified by Grieve et al. and Cambron further shows and discloses an apparatus including a terminal server connected between said network management system and said plurality of network components (in Carley reference, Fig. 17, SRMA block that acts as a terminal server, connecting each of the plurality of network components (router, servers etc.) of a data network via their non-network ports to the Network Management Station; paragraph 0089 which discloses that the SRMA can have multiple connections for accessing device consoles, thus acting like a terminal server).

Consider **claim 14**, and **as applied to claim 13 above,** Carley, as modified by Grieve et al., shows and discloses the claimed apparatus except explicitly disclosing that said terminal server in the claimed apparatus is configured to poll said plurality of network components.

In the same field of endeavor, Cambron clearly discloses that said terminal server is configured to poll said plurality of network components (column 7, lines 40-53 which disclose that SNMP network-management architecture includes a SNMP manager and a SNMP software agent that enable the network administrator to carry out network management functions by regularly polling and monitoring all SNMP devices in a network).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include capability that provided polling each of said network components, as taught by Cambron in the method of Carley, as modified by

Grieve et al., so that the network administrator can perform network management functions, such as fault, configuration, security, performance and accounting management at regular intervals.

Consider **claim 15**, and **as applied to claim 11 above**, Carley, as modified by Grieve et al. and Cambron, further discloses an apparatus wherein said data network ports comprise serial ports (in Carley reference, paragraphs 0088 and 0089 which disclose that the network management connection can be via the console port (as an RS-232 serial interface) of the network element).

Consider **claim 16**, and **as applied to claim 11 above,** Carley, as modified by Grieve et al. and Cambron, further discloses an apparatus wherein said data network ports comprise RS232 ports (in Carley reference, paragraphs 0088 and 0089 which disclose that the network management connection can be via the console port (as an RS-232 serial interface) of the network element).

Response to Arguments

Applicant's arguments filed 8/17/2007 with respect to **claims 1-5, 9-11 and 13-18** have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Art Unit: 2143

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Kishin G. Belani whose telephone number is (571) 270-1768. The Examiner can normally be reached on Monday-Thursday from 6:30 am to 5:00 pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, David Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 703-305-3028.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist/customer service whose telephone number is (571) 272-0800.

Kishin G. Belani

K.G.B./kgb

October 4, 2007

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100